



# Sovereign Bank

29

October 14, 2003

Two Aldwyn Center  
Lancaster Avenue & Route 320  
Villanova, PA 19085

Regulation Comments  
Chief Counsel's Office  
Office of Thrift Supervision  
1700 G Street NW  
Washington DC 20552  
Attn.: No. 03-35

VIA FACSIMILE

**RE: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice**

Dear Sir:

We respectfully submit for consideration the following observations on the above-captioned proposed guidance, in response to a number of the questions posed therein. We believe that much of what is recommended within the guidance is already being done, and, as such, our principal concern is with gaining some additional definition around the agencies' desires.

**Clarification of the Response Program Components.** We do not see a need for additional components to the program, merely better definition of those already proposed. We suggest that the term "unauthorized access" be defined with more specificity. It is unclear whether the program is to be limited to intentional unauthorized access, such as hacking, or is to be extended to inadvertent unauthorized access. Definitions of sensitive data, as has already been pointed out, can make the exchange of a signed check bearing an account number an unauthorized access. It is also unclear whether there are to be different standards applied to employees of the affected institution v. third parties.

**Notice in the event of unauthorized access.** Guidance on the general standards upon which an institution should reach conclusions regarding "likelihood of misuse" would be appropriate. We also suggest more specificity regarding the notification timing requirement. Customer notification should not be mandated before an adequate and accurate assessment of extent and occurrence can be accomplished.

**Anticipated burden of the notice provision.** We anticipate that the burden will most assuredly vary based upon the size and complexity of the institution. Larger institutions such as we have extended customer bases, spread over larger geographic footprints. Normal business patterns for an institution of larger size contain more opportunities for compromise, as data flows among service providers and over internet channels, as well as extended branch systems.

**"Securing the account."** It would be advisable to include what the specific regulatory expectations are in this regard, because the guidance as proposed is unclear.

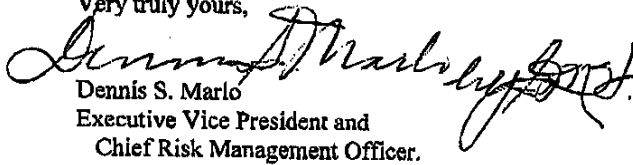
**Service Provider Contract Modifications.** Currently, we include obligations to comply with all privacy and information security guidelines as part of our standard contract language. We would expect to modify the requirements to provide for compliance with the final guidelines, so that there will be no misunderstandings about the expectations for discharging of regulatory obligations.

We believe that the initial focus of the response program should be on sensitive customer information. "Extraordinary circumstances," as suggested in the proposal, should be considered only after the current proposal has been implemented, and its consequences better understood. Overall, the Guidance, which tends to be somewhat "open-ended", should be expanded to include examples of the "unauthorized access" intended to be encompassed and/or excluded from the response program. Scenarios might be an

appropriate way to illustrate regulatory expectations, and permit financial institutions to focus on the specific violations with which the regulators are more concerned. Finally, we need more clarification regarding the SAR filing requirements in these regards, in terms of risk exposure and intent.

Thank you for this opportunity to offer our comments. Sovereign recognizes that identity theft is a deep and vital concern of our customers, and we are committed to assisting in eradicating this expensive and personally devastating crime.

Very truly yours,

  
Dennis S. Marlo  
Executive Vice President and  
Chief Risk Management Officer.